The Heritage Foundation
LEADERSHIP FOR AMERICA

ISSUE BRIEF

No. 3685 | JULY 30, 2012

Cybersecurity Legislation: Questions That Need to Be Answered

Paul Rosenzweig

The Senate has agreed to consider S. 3414, the Cybersecurity Act of 2012, this week. Before Senators vote on the bill or related amendments, such as the Whitehouse–Kyl "compromise" that raises many of the same issues, they should insist upon answers to the following questions.

Regulation. Title I would set up a "voluntary" regulatory structure to govern cybersecurity for "critical infrastructure." Here are some basic questions about this provision:

- **How much will it cost?** Given the complex structure of the bill, as well as pending amendments, nobody has been able to estimate what the costs will be to implement such a massive regulatory regime. The last-minute introduction of bills and Title I substitute amendments has not allowed for any vetting or even cost estimates by the Congressional Budget Office. Should the nation really give the federal government a blank check to impose new costs on businesses—the most dynamic sector of the economy?

- **What "critical infrastructure" is covered?** The bill and some proposed amendments will allow the Department of Homeland Security (DHS) to define what "critical infrastructure" is and how it will be covered. As of now, nobody knows which industries will fall under DHS's definition, creating even more uncertainty in the private sector during these already uncertain times.

- **Are the standards really voluntary?** If the standards really are voluntary, then why does section 103(g) of the bill allow the federal government to make the standards mandatory? And why are federal agencies required to justify a decision *not* to regulate instead of the normal process of justifying a decision *to* regulate?

- **Will the standards be outdated before they take effect?** Computer systems and processes are dynamic and change quickly to thwart threats. Every 18–24 months, processing capacity doubles. Yet major regulatory endeavors take around 36 months or more to complete. Will standards that take 36 months or longer to develop be relevant to an evolving dynamic industry?

- **Does the government have the requisite expertise?** Almost every report suggests that the government is short hundreds if not thousands of trained cyber specialists, as most qualified individuals take more lucrative jobs. The government is also facing its own serious cybersecurity challenges. Where will the government find enough qualified people to develop and implement any authorized regulations? How can the federal government, which cannot manage its own cybersecurity risks, be expected to do so for the private sector?

- **Can the federal government develop good standards?** The federal government has had more than 60 breaches of its own systems in the past eight years. What makes anyone think they would

This paper, in its entirety, can be found at **http://report.heritage.org/ib3685**

Produced by the Center for Legal & Judicial Studies

The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002
(202) 546-4400 | heritage.org

do better than the private sector, which is already doing a good job and has every incentive to do so?

- **Can DHS develop good regulatory standards?** The only other major regulation DHS has tried to implement, the Chemical Facility Anti-Terrorism Standards (CFATS), is mired in costly dysfunctionality. As of the end of 2011, nearly seven years after the CFATS program was authorized, not a single chemical facility has been able to complete the labyrinthine approval process. Will DHS do a better job with cybersecurity certification? Will private-sector resources be diverted to regulatory concerns rather than cybersecurity protection?

- **What will investors and innovators do?** While we are waiting for DHS or other agencies to develop "voluntary" cybersecurity standards, what will investors do? Would any wise investor put money into a project not knowing if it will be considered "critical infrastructure"? Will cybersecurity companies invest in creating new programs and technologies not knowing what the anticipated standards or requirements might be? This process could freeze investment and innovation for years.

- **Does the bill endanger the private sector's cybersecurity measures that are already in place?** Third-party audits of proprietary systems actually provide an opportunity for the creation of even more vulnerabilities. We have seen that the government cannot prevent its own information from leaking, so there is no guarantee that a third-party government auditor would provide adequate information security.

- **What about integrated systems?** Most major corporations have an integrated set of information systems, so the same system that runs a "critical" portion of the company is integrated with "non-critical" portions. This is entirely different from physical security, which often stops at the fence line. If a company has a facility that is deemed critical, will the entire company—in some cases a global or internationally based company—be subject to these regulations? Will the obligations apply overseas, where there may be contrary directives?

- **Why are information technologies carved out?** S. 3414 excludes from regulation "commercial information technology"—i.e., software. Regulating only the end user and not the developer is a bit like making the car owner responsible for fixing the flaws in the car instead of the manufacturer. This carve-out is very inappropriate and panders to one interest group.

- **Is there any reason to think that this approach would work?** The bill's supporters would be challenged to name a single recent incident that would have been prevented if new standards had been in place.

Information Sharing. Title VII of S. 3414 would authorize information sharing about cybersecurity threats and vulnerabilities, but there are still more questions that need to be answered:

- **Is information sharing limited?** Cyber threat information that is shared with the federal government can be used only for cyber purposes, such as to prevent imminent harm or to protect children from harm or exploitation. By re-erecting barriers and stovepipes, the bill returns to a pre-9/11 way of thinking. Why should federal law enforcement be prohibited from using lawfully obtained information to counter a nuclear threat? A bio threat? Mexican drug cartels? A terrorist attack on New York with bombs? A rape or murder?

- **Does the legislation actually encourage litigation?** The bill provides liability protection that protects nobody. It offers protections but then takes them away by allowing lawsuits for allegations of gross negligence. Anyone familiar with the tort system knows that this formulation will generate litigation, discovery costs, and coerced settlements. Furthermore, the bill creates a "damned if you do, damned if you don't" situation by failing to extend liability protection to actions taken as a result of information sharing while also allowing lawsuits for an entity's inaction. In the end, such provisions will only disincentivize the sharing of critical threat and vulnerability information.

How Washington Could Help. Government can help improve cybersecurity by improving information sharing, increasing public awareness

and education, increasing already established public-private partnerships, and ensuring that government systems are protected and harmonized. The creation of a regulatory leviathan and a system designed to encourage litigation over information sharing would do more harm than good.

*—**Paul Rosenzweig** is a Visiting Fellow in the Center for Legal and Judicial Studies and the Douglas and Sarah Allison Center for Foreign Policy Studies, a division of the Kathryn and Shelby Cullom Davis Institute for International Studies, at The Heritage Foundation.*